AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (Previously Presented) A method of performing point doublings in a computing system comprising:

generating a first point doubling using an initial point (x, y) comprising generating a current slope value and a current x value;

generating a second point doubling comprising generating a new current slope value with at least one square operation without computing a y coordinate, and generating a new current x value with the new current slope value.

2. (Original) The method of claim 1 wherein said generating said second point doubling comprises generating a new current x value and new current slope value without using a y term.

3. (Original) The method of claim 1 wherein said generating said second point doubling comprises storing said current x value as a prior x value and storing said current slope value as a prior slope value; generating a new current x value using said prior slope value; and generating a new current slope value using said new current x value and said prior x value.

4. (Original) The method of claim 3 wherein said new current x value is generated by:

$x_1 = s^2 + s + a$

where s is said prior slope value.

5. (Original) The method of claim 3 wherein said new current slope value is generated by:

$g = (x + x_1)^2 / x_1 + (s+1)$

where x is said prior x value and x1 is said current x value.

6. (Previously Presented) A method of generating an *n*th point doubling for a point (x_0, y_0) for a security value, the method comprising:

generating an initial slope with $\text{slope}_1 = x_0 + y_0/x_0$;

generating an initial x_1 with $\text{slope}_1^2+\text{slope}_1+A$, wherein A is a constant;

generating successive slopes with $\text{slope}_i = (x_{i-2}+x_{i-1})^2/x_{i-1} + (\text{slope}_{i-1} + 1)$, wherein i corresponds to succession;

generating successive x values with $x_i = (\text{slope}_i)^2 + \text{slope}_i + A$;

generating a final y value for the *n*th point doubling with $y_n = x_{n-1}^2 + (\text{slope}_n + 1)*x_n$; and

supplying the final y value and the final x value for generation of a security value.

7. (Previously Presented) The method of claim 6 wherein the security value includes one or more of an encryption key and a value to determine an encryption key.

8. (Previously Presented) The method of claim 7 wherein generation of the *n*th point doubling is performed with squares and reciprocals and without multiplication.

9. (Previously Presented) The method of claim 6 wherein the successive slopes and the successive x values are generated without a y value.

10. (Previously Presented) The method of claim 6 wherein the point (x_0, y_0) is an element of a field $F(_2m)$, wherein the x coordinate and the y coordinate are represented with *m*-bit strings.

11. (Previously Presented) The method of claim 6 embodied as a computer program product, encoded on one or more machine readable media.

12. (Currently Amended) A method of generating a security value comprising:

repeatedly performing reciprocals and squares to determine successive x values and successive slopes for *n* point doublings of a point (x, y), wherein the ~~reciprocals are used to determine~~ successive slopes <u>are determined in accordance with slope_i</u>

$= (x_{i-2}+x_{i-1})^2/x_{i-1} + (slope_{i-1} + 1)$ and the ~~squares and~~ successive x values ~~slopes~~ are determined in accordance with $x_i = (slope_i)^2 + slope_i + A$, wherein i corresponds to succession ~~used to determine successive x values~~; and

generating y_n from x_n , x_{n-1}, and $slope_n$, wherein x_n, x_{n-1}, and $slope_n$ have been determined with one or more preceding x values and one or more preceding slopes, wherein *n* corresponds to the number of point doublings.

13. (Currently Amended) The method of claim 12 further comprising decomposing a scalar multiplication Q = kP into point additions and repeated point doublings, which at least include the *n* point doublings, wherein P is represented by the coordinates (x, y).

14. (Previously Presented) The method of claim 13 further comprising separating k into zero windows and non-zero windows.

15. (Previously Presented) The method of claim 13 further comprising looking up the point additions in a look-up table.

16. (Previously Presented) The method of claim 13 wherein Q and P are security values for elliptic curve cryptography.

17. (Cancelled)

18. (Previously Presented) The method of claim 12 wherein the y_n is generated with $y_n = x_{n-1}^2 + (slope_n + 1)*x_n$.

19. (Previously Presented) The method of claim 12 embodied as a computer program product encoded on one or more machine-readable media.

20 – 26. (Cancelled)

27. (Previously Presented) An apparatus comprising:

memory; and

means for performing repeated point doublings with successive slopes based on slopes and x values of preceding point doublings, but without y values, and successive x values based on corresponding ones of the successive slopes.

28. (Previously Presented) The apparatus of claim 27 wherein the memory hosts pre-computed point additions.

29. (Previously Presented) The apparatus of claim 27 further comprising means to decompose a scalar multiplication into one or more point doublings.

30. (Previously Presented) The apparatus of claim 29 further comprising means to decompose the scalar multiplication into point additions.